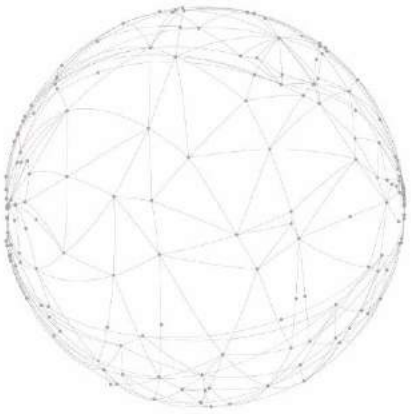
云计算开源产业联盟
OpenSource Cloud Alliance for industRy,OSCAR

开 源 产 业 白 皮 书

（2019年）

云计算开源产业联盟

2019年7月



版权声明

前　言

当前开源技术快速发展，在云计算、大数据、人工智能等领域逐渐形成技术主流，开源技术已经成为企业构建信息系统的重要选择，国内企业参与开源生态的热情度持续提升。开源一方面可以突破技术壁垒，推动技术创新，另一方面也面临知识产权、安全、技术运维等一系列与开源相关的风险问题。抓住开源技术的快速发展机遇，有必要进一步健全开源生态、树立开源风险意识、加强开源治理，推动我国开源产业健康快速发展。

《开源产业白皮书》首先通过调查问卷的形式梳理了开源软件市场总体规模及应用现状，然后从知识产权及合规、安全、技术运维三个角度分别对开源软件的风险进行调查分析，进一步总结开源产业发展特点及趋势，最后结合当前现状给出了我国开源产业发展建议。

本白皮书采用电话访谈和在线调查相结合的方式，共回收有效问卷 4,135 份，同时利用代码扫描工具对软件的组件、许可证、漏洞等情况进行统计。在数据采集、代码扫描及编写过程中得到了 FOSSID 等扫描工具和中国 IDC 圈的支持。

目 录

一、全球开源软件市场规模及应用现状.....1
（一）开源产业链条逐渐形成.....1
（二）全球开源软件市场现状.....2
（三）我国开源技术市场应用现状.....3
1、企业对开源技术的接受程度逐年增高.....3
2、开源解决方案是企业的重要关注点.....4
3、联合开发成为企业部署开源的主要选择.....6
4、企业应用开源技术仍面临众多挑战.....6
（四）我国云计算相关开源技术应用现状.....7
1、容器技术应用持续深化.....7
2、虚拟化技术走向成熟期.....10
3、微服务应用逐步落地.....12
4、DevOps 进入实践阶段.....14
二、开源软件风险调查分析.....15
（一）知识产权及合规风险.....16
1、风险分析.....16
2、调查结果.....17
（二）安全风险.....22
1、风险分析.....22
2、调查结果.....23
三、我国开源产业发展特点及趋势.....28
四、我国开源产业发展建议.....29
附录：开源软件风险调查扫描软件清单.....30

一、全球开源软件市场规模及应用现状

（一）开源产业链条逐渐形成

开源即开放一类技术或一种产品的源代码，源数据，源资产，可以是各行业的技术或产品，其范畴涵盖文化、产业、法律、技术等多个社会维度。如果开放的是软件代码，一般被称作开源软件。开源经过形成时期、古典时代、移动时代到云开源时代的不断发展，开源产业链条已经逐渐形成，其中涉及的企业类型包括：**自发开源企业**、**开源产品企业**和**开源用户企业**。

图 1 开源产业链条构成

自发开源企业指对开源社区做出贡献的企业，如将企业内已有代码形成项目，公开发布于代码托管平台或捐赠给开源基金会，其代码能够被公开获取。著名的开源项目如 Android、Linux、TensorFlow 等，背后多为谷歌、微软等科技公司。近年来国内华为、腾讯、阿里等企业均积极主动发起开源项目，主要集中在云计算、大数据、存储、运维等领域，在国际上的影响力逐渐提升。

开源产品企业指基于社区版开源软件提供发行版售卖给开源用户企业，或针对主流社区版开源软件提供服务（包括：软件选型咨询、软件运维服务支持等）的企业。

开源用户企业指从开源社区获取开源软件或代码，用于自身信息系统构建以辅助实现企业前台业务功能的机构，包括诸多传统行业，

如金融、电力、通信、能源等。据 Gartner 调查显示，99%的组织在其 IT 系统中使用了开源软件，随着开源技术快速形成生态，企业用户引入开源技术已成大势所趋。

（二）全球开源软件市场现状[1]

全球开源热度持续攀升。截至 2018 年，全球最大的代码托管平台 GitHub 已有 3000 万开发人员，其中 2018 年的新用户数量超过了前六年用户数之和；囊括 200 万家企业或组织，2018 年的组织数目比去年增加了 40%；拥有 9600 万个代码库，超过三分之一的代码库是在 18 年创建的；已提交 2 亿的 pull request，仅在过去一年就创造了超过 6000 万次。

中国贡献者在开源社区中持续活跃。截至 2018 年，全球最大的代码托管平台 GitHub 上超过 80%的用户来自美国以外的地区，其中中国的贡献者数目仅次于美国，排名第二；2018 年 GitHub 上的贡献者数量是 2017 年的 1.6 倍，其中中国的新注册用户数目仅次于美国，排名第二。

热门领域开源项目涌现，公司成为开源的重要贡献者。2018 年，JavaScript（前端和后端）、机器学习、移动应用程序开发和容器是贡献最多的领域。其中，微软 VS Code、Facebook React、谷歌 TensorFlow 位列项目活跃度前三甲(按贡献者数目排序)。整体来看，微软、谷歌、红帽、英特尔等顶级科技公司的员工是开源项目的重要贡献者。

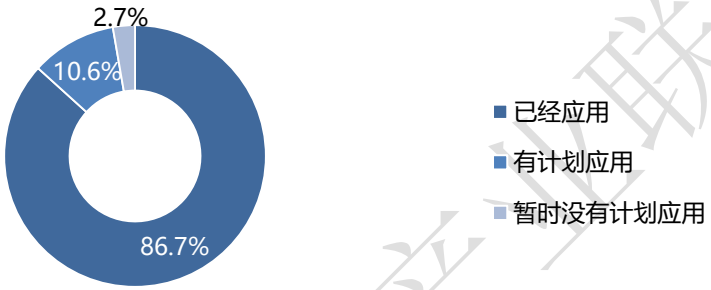
[1] 数据来源：https://octoverse.github.com/

（三）我国开源技术市场应用现状

1、企业对开源技术的接受程度逐年增高

超过八成的企业认可开源技术。调查显示，已经应用了开源技术的企业占比达到 86.7%，有计划应用开源技术的企业占比 10.6%，开源技术已经被企业普遍接受。

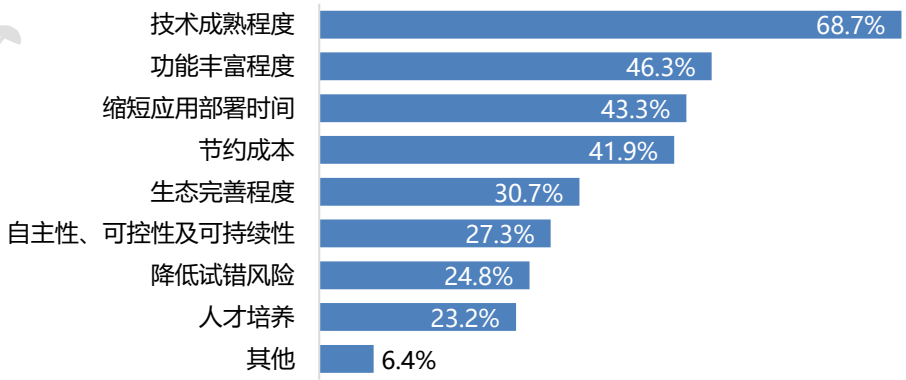
图 2 2018 年开源技术使用率调查（N=4135）



数据来源:中国信息通信研究院

技术成熟程度和功能丰富度是企业选择开源技术时考虑的重要因素。据调查，企业对技术成熟度的关注最高，达到 68.7%；其次，46.3%的企业在选择开源技术时会考虑功能丰富程度。此外，还有 43.3%的企业因缩短应用部署时间而选择开源技术。

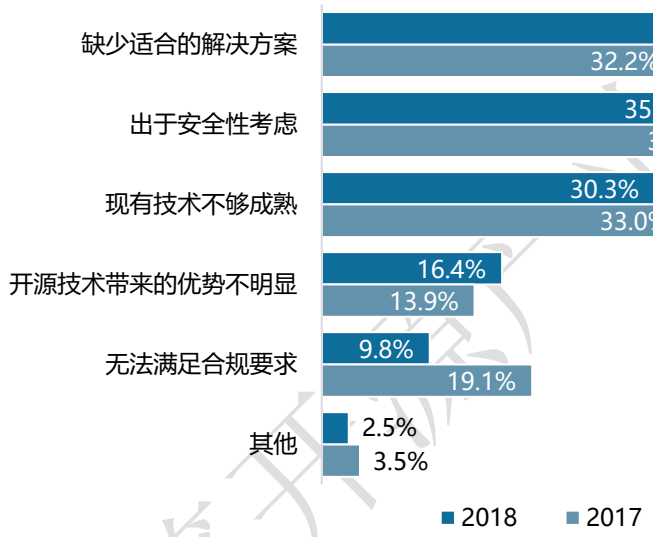
图 3 企业选择开源技术的考虑因素（N=4023）



数据来源:中国信息通信研究院

缺少适合的解决方案和出于安全性考虑是企业尚未应用开源技术的两个原因。在尚未应用开源技术的企业中，认为缺少适合的解决方案的企业占比最高，达到 43.4%，与去年相比提高了 11.2%；其次，有 35.2%的企业出于安全性考虑尚未使用开源技术。其他因素还包括：现有技术不够成熟（30.3%）、开源技术带来的优势不明显（16.4%）以及无法满足合规要求（9.8%）。

图 4 企业尚未应用开源技术的原因（N=550）

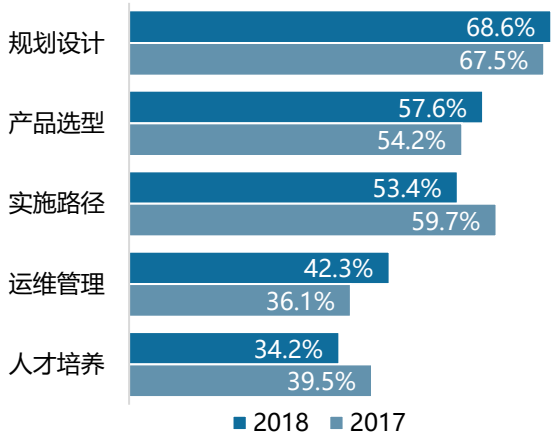


数据来源:中国信息通信研究院

2、开源解决方案是企业的重要关注点

规划设计和产品选型是最受企业关注的解决方案类型。据调查，企业对于规划设计类解决方案的需求最为强烈，占比达到了 68.6%，相比 2017 年上升了 1.1 个百分点；其次，57.6%的企业更关注产品选型，比去年提高了 3.4%。其他开源解决方案还包括实施路径、运维管理和人才培养等。

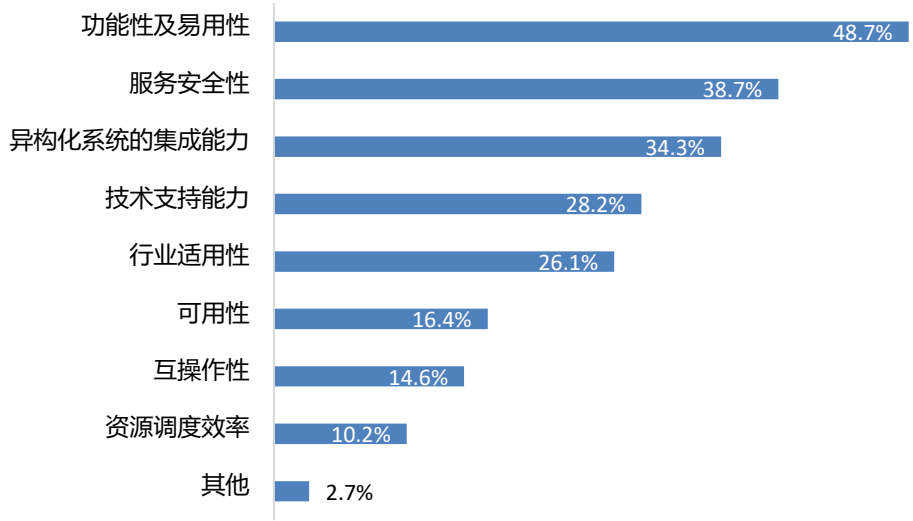
图 5 企业对开源解决方案的选择（N=4023）



数据来源:中国信息通信研究院

开源解决方案的功能性及易用性和服务安全性是企业的首要关注点。在企业对开源解决方案关注指标的调查中，有 48.7%的企业更注重功能性及易用性，占比最高；其次，分别有 38.7%和 34.3%的企业更关注服务安全性和异构化系统的集成能力。其他受关注的指标还包括：技术支持能力（28.2%）、行业适用性（26.1%）以及可用性（16.4%）等。

图 6 企业对开源解决方案的关注指标（N=4023）

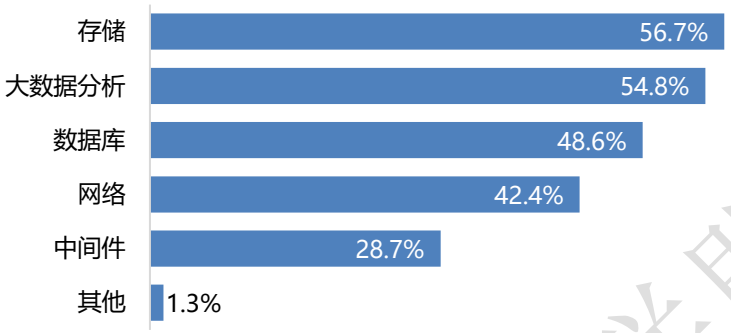


数据来源:中国信息通信研究院

存储是企业开源技术的首要应用方向。调查显示，将开源技术应

用于存储领域的企业占比最高，达到 56.7%；其次是大数据分析（54.8%）。其他应用方向还包括：数据库、网络和中间件。

图 7 企业开源技术应用方向（N=4023）

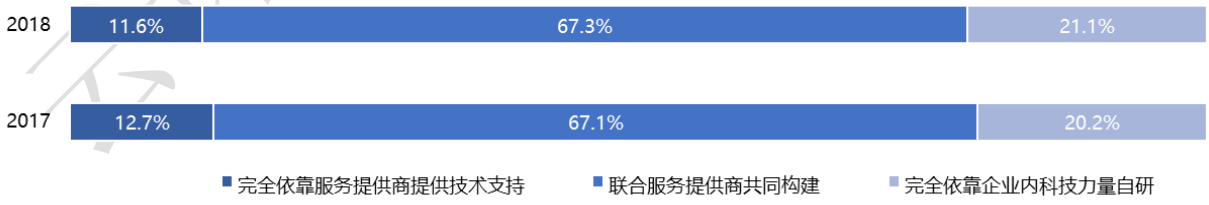


数据来源:中国信息通信研究院

3、联合开发成为企业部署开源的主要选择

近七成的企业选择联合服务商共同实施开源技术。在企业云计算开源技术实施方式的调查中，选择联合服务商共同实施开源技术的企业比例最高，达到 67.3%；其次，21.1%的企业选择完全依靠企业内部科技力量自研，这与 2017 年相比提高了 0.9 个百分点。

图 8 企业开源技术实施方式（N=4023）



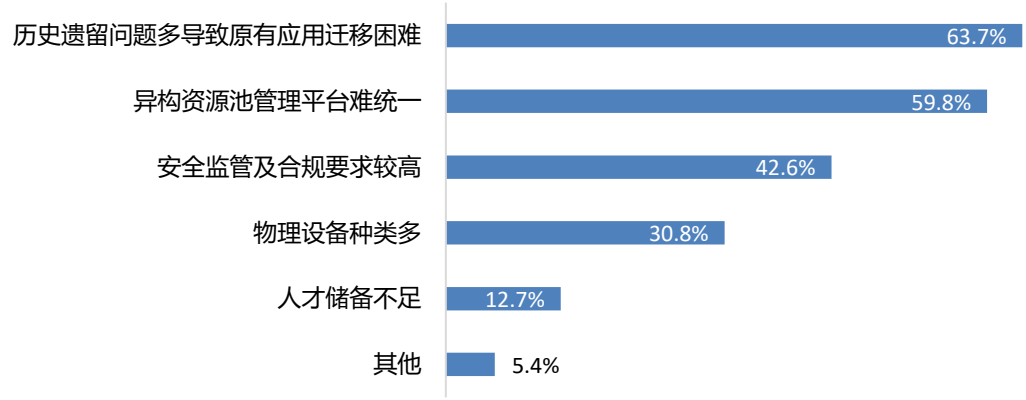
数据来源:中国信息通信研究院

4、企业应用开源技术仍面临众多挑战

历史遗留问题多、异构资源池管理平台难统一、安全监管以及合

规要求较高是企业应用开源技术面临的重要挑战。历史遗留问题多是企业应用开源技术面临的最大困难，占比达到 63.7%；其次 59.8%的企业认为异构资源池管理平台难以统一。此外，分别有 42.6%和 30.8%的企业表示安全监管以及合规要求较高、物理设备种类多是其应用开源技术面临的挑战。

图 9 企业应用开源技术面临的挑战（N=4135）



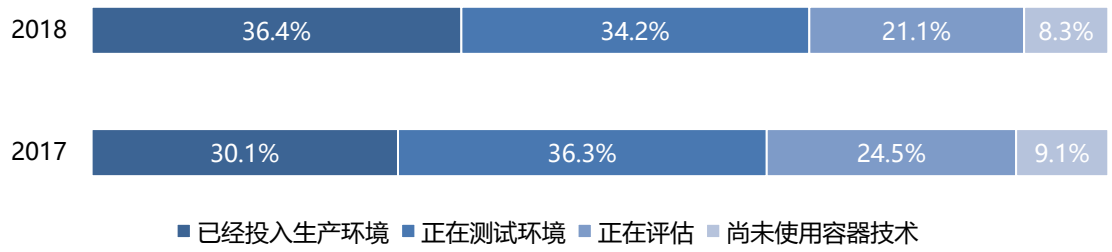
数据来源:中国信息通信研究院

（四）我国云计算相关开源技术应用现状

1、容器技术应用持续深化

超过七成的企业已经使用容器技术或正在测试应用环境。据调查，36.4%的企业已经使用了容器技术，相比 2017 年提高了 6.3%；其次，正在测试容器技术应用环境的企业占比达到 34.2%，比去年减少了 2.1 个百分点。此外，还有 21.1%的企业正在评估容器技术。

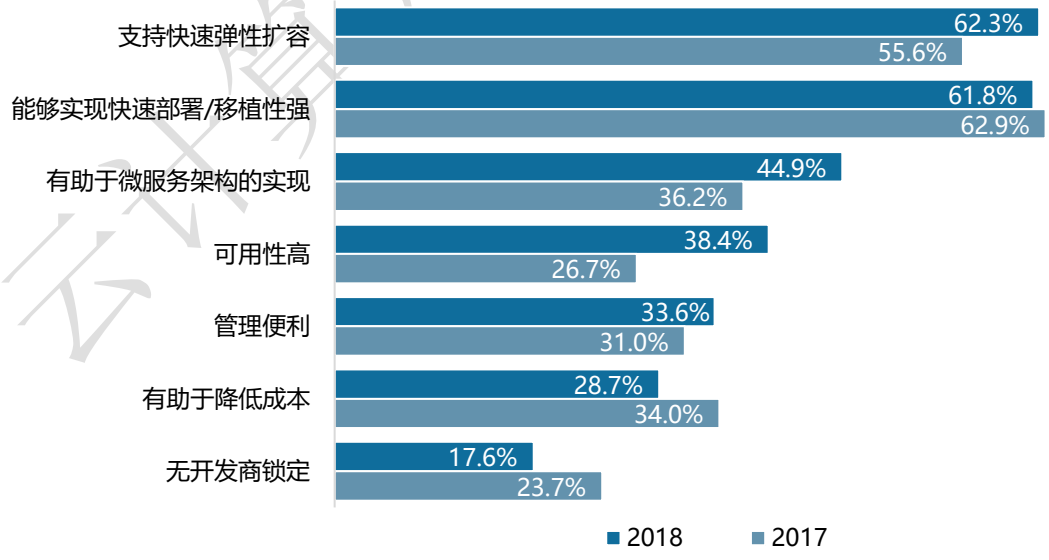
图 10 云计算容器技术使用阶段（N=918）



数据来源:中国信息通信研究院

支持快速弹性扩容和移植性强是企业选择容器技术的优先考虑因素。调查显示，出于支持快速弹性扩容和能够实现快速部署/移植性强考虑而应用容器技术的企业占比分别达到 62.3%和 61.8%；其次，有 44.9%的企业认为容器技术有助于微服务框架的实现，相比 2017 年提高了 8.7%。另外，可用性高（38.4%）以及管理便利（33.6%）也是企业应用容器技术的主要推动力。

图 11 企业应用云计算容器技术的原因（N=648）

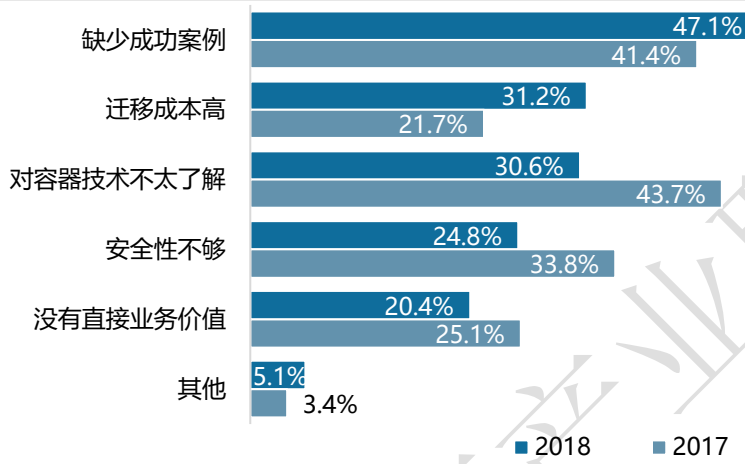


数据来源:中国信息通信研究院

缺少成功案例是企业应用容器技术面临的最大挑战。调查显示，

出于缺少成功案例的原因而未使用容器技术的企业占比为 47.1%；其次，迁移成本高和对容器技术不太了解也是企业未使用容器技术的重要因素，占比分别为 31.2%和 30.6%。根据访谈，企业对成功案例和迁移成本的关注程度有所上升。

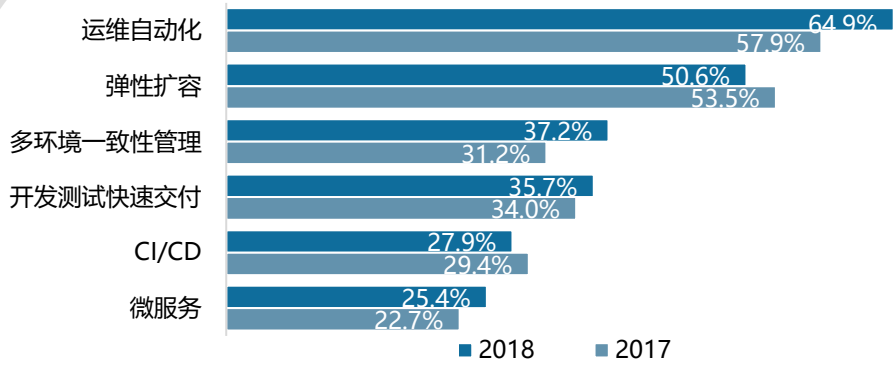
图 12 企业尚未应用云计算容器技术的原因（N=584）



数据来源:中国信息通信研究院

运维自动化和弹性扩容是容器技术应用最多的两个场景。在企业容器技术应用场景的调查中，64.9%的企业选择将容器技术用于运维自动化，相比 2017 年上升了 7.0%；其次，应用容器技术实现弹性扩容的企业占比达到 50.6%。此外，企业还将容器技术应用在多环境一致性管理和开发测试快速交付等场景中。

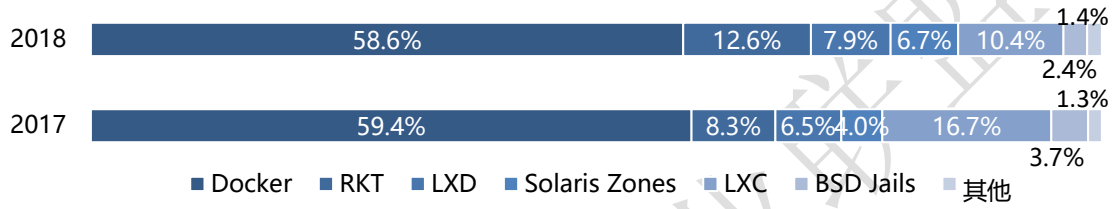
图 13 企业云计算容器技术应用场景（N=648）



数据来源:中国信息通信研究院

近六成的企业选择 Docker 作为容器运行技术。调查显示，在已经应用容器技术的企业中，选择 Docker 的企业占比最高，达到 58.6%；在众多技术中，RKT 与去年相比增幅最大（4.3%）。其他容器技术还包括：LXD、Solaris Zones 和 LXC 等。

图 14 企业云对计算容器运行技术的选择（N=648）

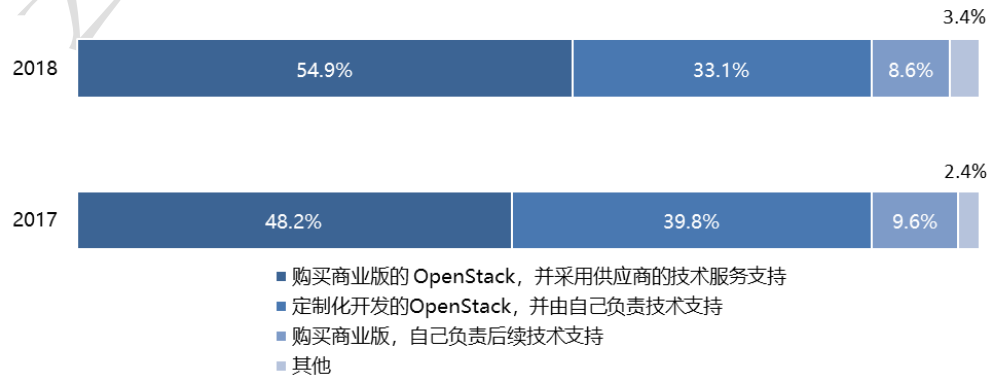


数据来源:中国信息通信研究院

2、虚拟化技术走向成熟期

超过半数的企业选择购买商业版 OpenStack，并采用供应商的技术服务支持。在 OpenStack 解决方案选择的调查中，54.9%的企业选择购买商业版的 OpenStack 并采用供应商的技术服务支持，相比 2017 年上升了 6.7%。此外，还有 33.1%的企业选择定制化开发 OpenStack，并自己负责技术支持。

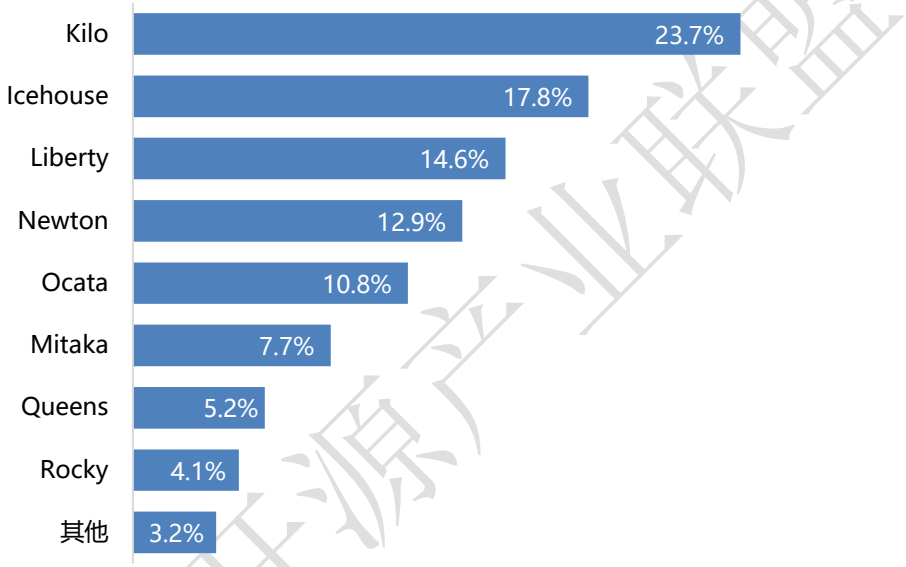
图 15 云计算 OpenStack 解决方案选择（N=603）



数据来源:中国信息通信研究院

Kilo 和 Icehouse 是企业应用较为广泛的两个 OpenStack 版本。调查显示，最受企业欢迎的版本是 Kilo，占比达到 23.7%；选择 Icehouse 版本的企业达到 17.8%；其次，分别有 14.6%和 12.9%的企业使用了 Liberty 和 Newton 版本。其他受关注的 OpenStack 版本还包括 Ocata、Mitaka 和 Queens 等。

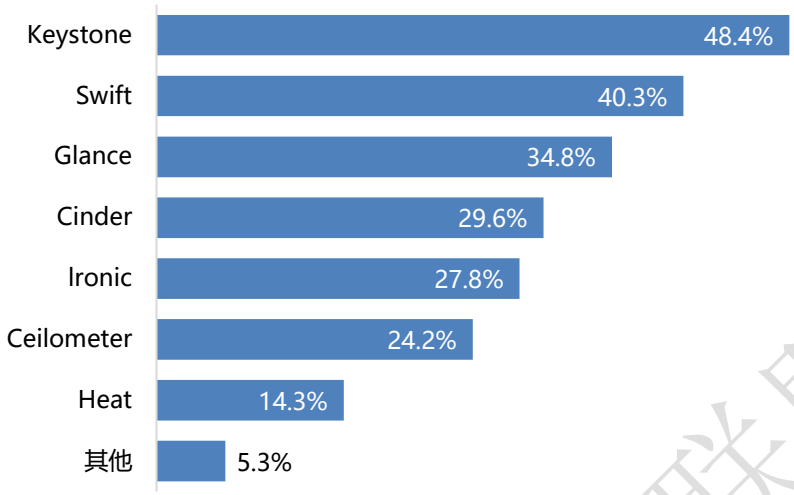
图 16 2018 年云计算 OpenStack 版本选择 (N=603)



数据来源:中国信息通信研究院

在众多组件中，Keystone 最受企业欢迎。使用 Keystone 组件的企业占比最高，达到 48.4%；其次，分别有 40.3%和 34.8%的企业应用了 Swift 和 Glance 组件。其他 OpenStack 组件还包括：Cinder（29.6%）、Ironic（27.8%）、Ceilometer（24.2%）和 Heat（14.3%）等。

图 17 企业应用的云计算 OpenStack 组件（N=603）

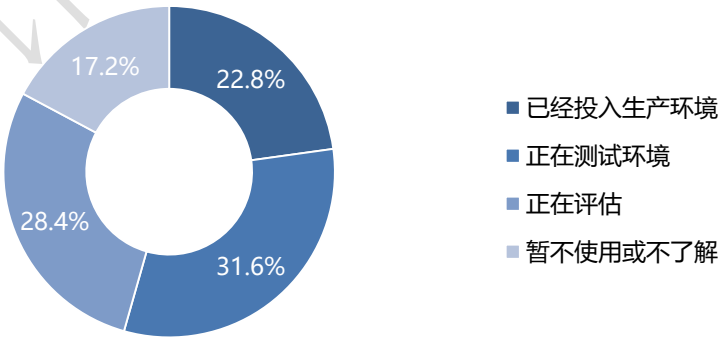


数据来源:中国信息通信研究院

3、微服务应用逐步落地

超过六成的企业已经应用或正在测试微服务框架。在对企业微服务框架使用情况的调查中发现，22.8%的企业已经应用了微服务框架；其次，正在测试环境的企业占比达到了 31.6%；此外，还有 28.4%的企业正在评估微服务框架。

图 18 云计算微服务框架使用接受程度（N=918）

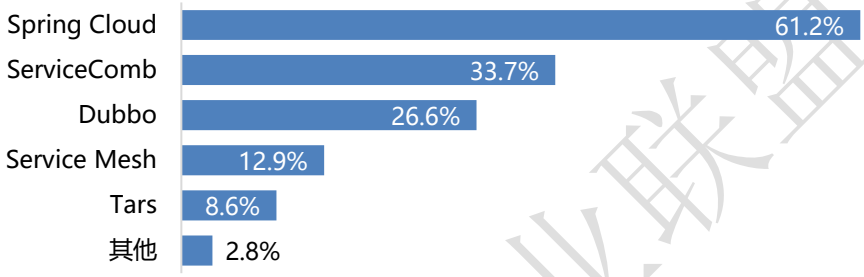


数据来源:中国信息通信研究院

超过六成的企业选择 Spring Cloud 作为其微服务框架。据调查，

选择 Spring Cloud 作为微服务框架的企业比例最高，达到 61.2%；其次，有 33.7%的企业认为 Service Comb 更适合作为其微服务框架。其他受关注的微服务框架还包括：Dubbo（26.6%）、Service Mesh（12.9%）和 Tars（8.6%）。

图 19 企业对云计算微服务框架的选择（N=499）



数据来源:中国信息通信研究院

缺乏运维人员和改造成本较高是企业未使用微服务框架的两个重要原因。调查发现，因缺乏运维人员而未使用微服务框架的企业占比达到 39.3%；其次，有 33.5%的企业认为改造成本较高是其未使用微服务框架的主要原因。此外，分别有 31.8%和 26.9%的企业未使用微服务框架的原因是业务暂时不需要和技术人员缺乏了解。

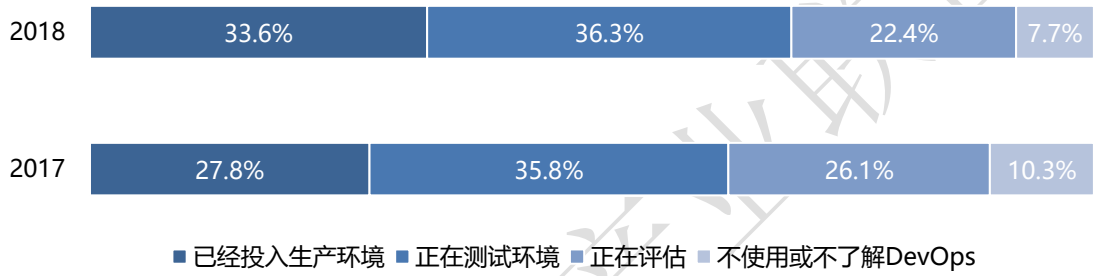
图 20 企业尚未应用云计算微服务框架的原因（N=709）

数据来源:中国信息通信研究院

4、DevOps 进入实践阶段

超过 1/3 的企业已经实现了系统的自动化运维。对 DevOps 应用阶段的调查显示，33.6%的企业表示已经投入生产环境，与 2017 年相比提高了 5.8%；其次，36.3%的企业表示正在测试环境。此外，尚未考虑使用 DevOps 的企业仅有 7.7%。

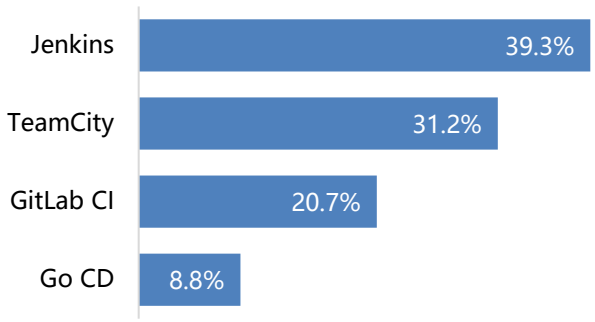
图 21 企业云计算 DevOps 实现情况（N=918）



数据来源:中国信息通信研究院

Jenkins **是目前企业使用最广泛的开源集成工具。**调查发现，在诸多开源集成工具中，Jenkins 的使用比例最高，达到 39.3%；其次，分别有 31.2%和 20.7%的企业表示已经应用了 TeamCity 和 GitLab CI。此外，使用 Go CD 的企业占比为 8.8%。

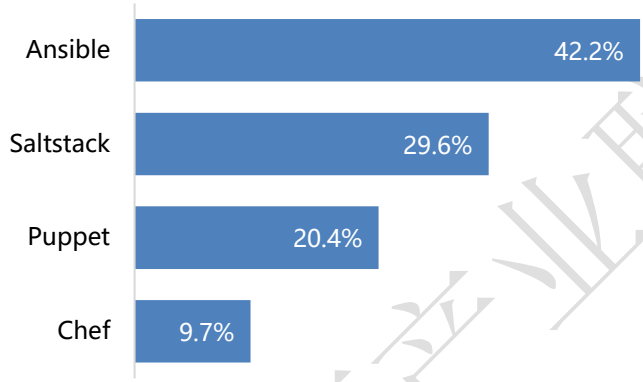
图 22 企业云计算开源集成工具使用情况（N=642）



数据来源:中国信息通信研究院

超过四成的企业将 Ansible 作为自动化运维工具。调查发现，Ansible 是企业使用率最高（42.2%）的自动化运维工具；此外，还有29.6%的企业选择了 Saltstack。其他受关注的自动化运维工具还包括： Puppet（20.4%）和 Chef（9.7%）。

图 23 企业云计算开源自动化运维工具使用情况（N=642）



数据来源:中国信息通信研究院

二、开源软件风险调查分析

相比于闭源软件，开源软件的代码公开、获取便捷，但企业和个人在使用开源软件的过程中仍需注意遵循相关规则，包括开源许可证的要求、开源基金会的规范、甚至相关国家法律条例等。由于开源软件的所有权和使用权分离，导致用户往往成为开源的风险落脚点，因此用户在引入和使用开源软件的过程中应充分重视潜在风险问题。

总体来看，开源软件可能涉及三类风险：**知识产权及合规风险、安全风险、运维和技术风险**，其中，知识产权及合规风险主要与开源许可证的规定相关，安全风险主要涉及安全漏洞等问题，运维和技术风险主要指因开源软件的引入导致的开发运维投入量大、技术人员要

求高等问题。针对前两项风险，本白皮书通过代码扫描的方式，对若干热门开源软件的实际风险情况进行了调查和统计。

（一）知识产权及合规风险

1、风险分析

除法律法规的保护外，开源软件的作者或权利人主要是通过开源许可证对其知识产权进行许可与约束。若开源软件使用者未依照相应的开源许可证来使用开源软件，将可能侵犯开源软件的作者或权利人的知识产权。

目前经过 Open Source Initiative（以下称“OSI”）认证的开源许可证共有 83 种。根据其传染型强弱大致可以分为四类：

表 1 常见开源许可证分类

许可证类型	许可证名称	版本
开放型许可证 (Permissive License)	MIT license	/
	BSD 2-Clause	2-Clause
	BSD 3-Clause	3-Clause
	Apache License	2.0
弱传染型许可证 (Weak Copyleft License)	GNU LGPL	2.1
	GNU LGPL	3.0
	Mozilla Public License (MPL)	2.0
	Eclipse Public License (EPL)	1.0
传染型许可证 (Copyleft License)	GNU GPL	2.0
	GNU GPL	3.0

强传染型许可证 (Strong Copyleft License)	GNU AGPL	3.0

个人或企业在使用开源软件时，因开源许可证的规定或变动，可能面临知识产权及合规风险，一是可能因许可证的传染性规定被迫开源，如：根据 GPL 许可证的规定，使用依 GPL 开源的软件并涉及到修改和分发，需要将后续修改代码全部开源；二是商业软件是否遵守开源约定未知，如：部分商业软件基于开源进行二次开发后以闭源形式提供给用户，却不遵守开源许可证的署名要求；三是知识产权风险易被忽略，如：BSD、MIT 和 GPL 2.0 等并未明确包含明确的专利许可条款，许可用户使用软件所包含的相关专利；四是开源许可证之间可能不兼容，如：GPL 开源许可证在 GNU 的网站上详细列出何种开源许可证是否与其兼容[2]；五是开源软件的使用规则存在不确定性，如：2018 年以来多个开源软件开发商（Redis 、MongoDB、Kafka 等）已经对其过去使用的开源许可证进行了修改，Oracle 宣布 2019 年 1 月以后发布的 Oracle Java SE 8 公开更新将不向没有商用许可证的业务、商用或生产用途提供。

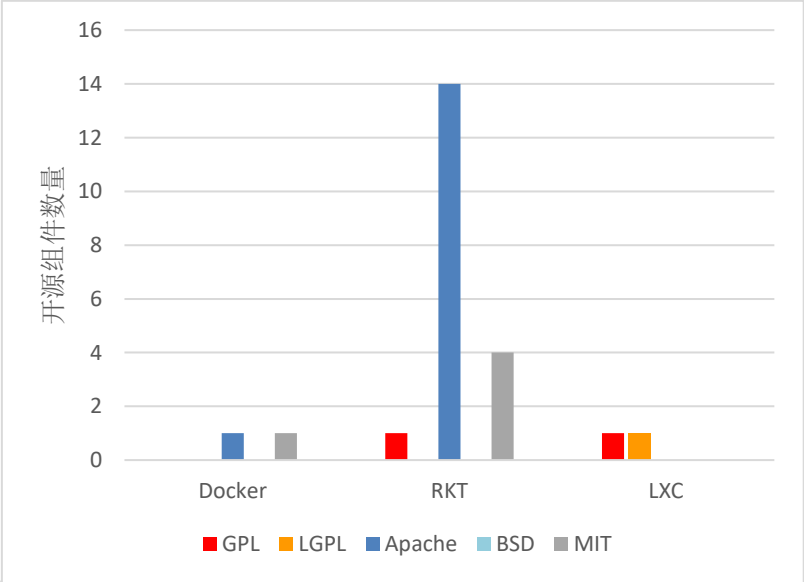
2、调查结果

本白皮书利用工具对软件源代码进行扫描，设置规则为：若被扫描软件中有超过 5 个文件与开源组件库中的组件匹配，即认定可能包含该开源组件。然而，受开源组件库完整度和更新频率限制，且算法匹配过程中可能存在误差，本白皮书调查结果仅供参考。

[2] https://www.gnu.org/licenses/license-list.en.html#GPLIncompatibleLicenses

热门开源容器运行技术存在隐含风险，RKT 和 LXC 均发现少量使用传染性许可证的开源组件。本白皮书对企业选择最多的三个开源容器运行技术（Docker、RKT 和 LXC）进行扫描，结果显示：Docker 暂未发现使用传染性许可证的开源组件，RKT 和 LXC 中发现少量使用传染性许可证的开源组件。其中，RKT 包含 1 个使用 GPL 许可证的开源组件，LXC 包含 1 个使用 GPL 许可证的开源组件和 1 个使用 LGPL 许可证的开源组件。

图 24 热门开源容器技术许可证情况调查



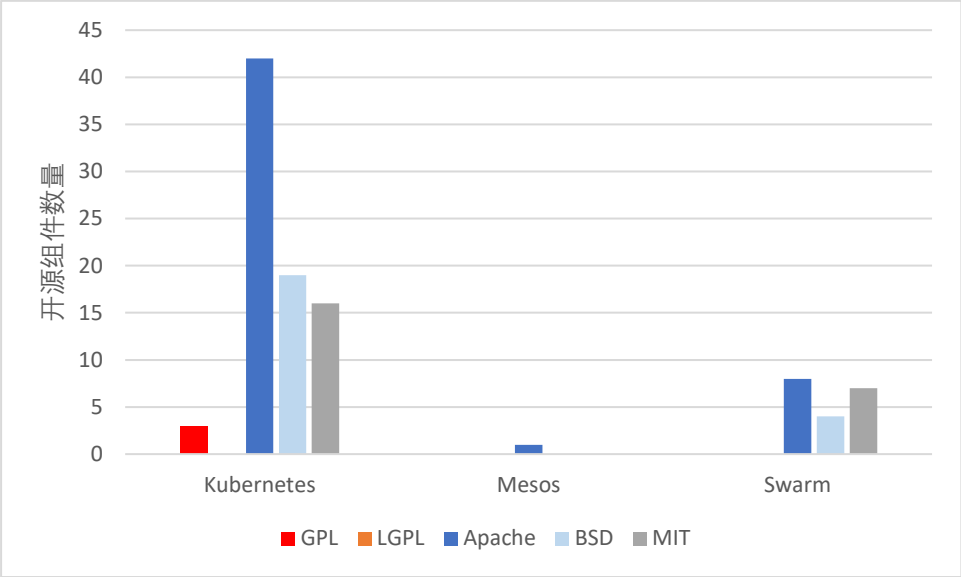
软件名称	许可证类型	组件名称（带有传染性的许可证名称）
Docker	Apache-2.0	/
RKT	Apache-2.0	go(GPL-2.0)
LXC	LGPL-2.1	jdk(GPL-2.0) lxc(LGPL-2.1)

数据来源:中国信息通信研究院

热门开源容器编排技术中，Kubernetes 发现少量使用传染性许可证的开源组件。本白皮书对企业选择最多的三个开源容器编排技术（Kubernetes、Mesos 和 Swarm）进行扫描，结果显示：Mesos 和 Swarm

暂未发现使用传染性许可证的开源组件，Kubernetes 中发现 3 个使用 GPL 许可证的开源组件。

图 25 热门开源容器编排技术许可证情况调查

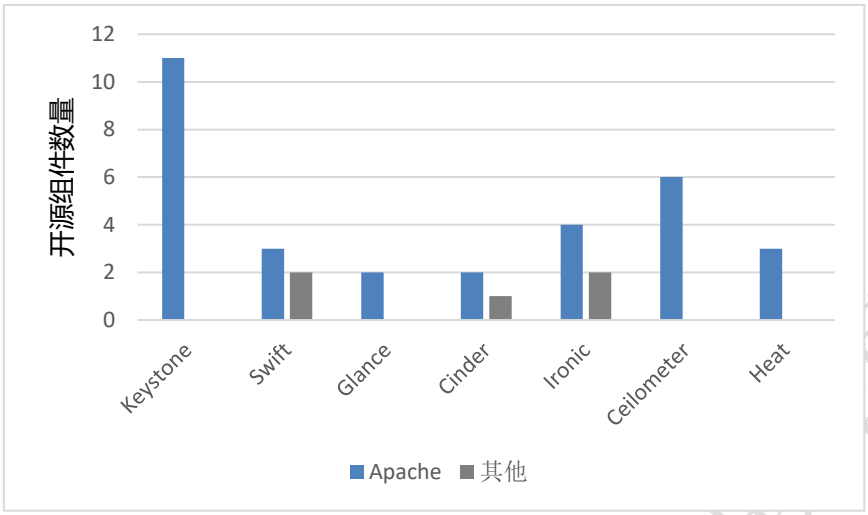


软件名称	许可证类型	组件名称（带有传染性的许可证名称）
Kubernetes	Apache-2.0	heketi(GPL-3.0) duplicatecheck(GPL-3.0) goproxy(GPL-2.0)

数据来源:中国信息通信研究院

OpenStack 的 7 大常用组件未发现传染性许可证。本白皮书对 7 个 OpenStack 常用组件进行扫描，结果显示：以上组件主要应用的许可证是 Apache 2.0，其中 Swift、Ironic、Cinder 等开源组件也包含其他的许可证，如：MIT 和 ECL-2.0。

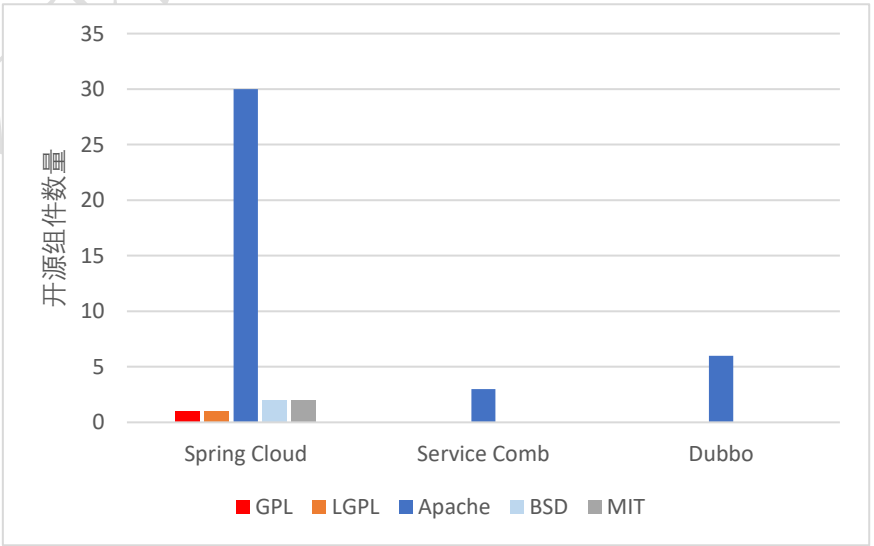
图 26 OpenStack 常用组件许可证情况调查



数据来源:中国信息通信研究院

热门开源微服务框架中，Spring Cloud 发现使用传染性许可证的开源组件。本白皮书对企业选择最多的三个开源微服务框架技术（Dubbo、Service Comb 和 Spring Cloud）进行扫描，结果显示：Dubbo 和 Service Comb 中暂未发现使用传染性许可证的开源组件，其主要许可证是 Apache 2.0。Spring Cloud 的众多组件中发现 1 个使用 GLP 许可证和 1 个使用 LGLP 许可证的开源组件。

图 27 热门开源微服务框架许可证情况调查

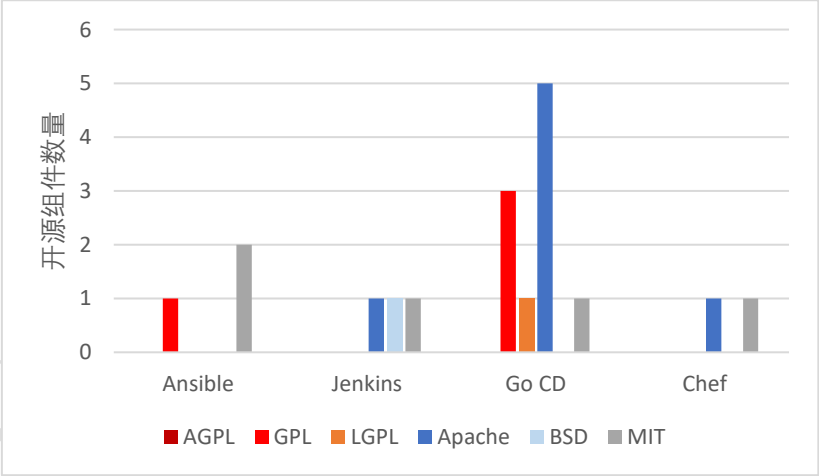


软件名称	许可证类型	组件名称（带有传染性的许可证名称）
Spring Cloud	Apache-2.0	git(GPL-2.0+) postgresql-mingw-w64(LGPL-3.0)
Service Comb	Apache-2.0	/
Dubbo	Apache-2.0	/

数据来源:中国信息通信研究院

DevOps 领域热门开源软件所含组件的许可证情况较为复杂，隐含风险需引起关注。本白皮书对企业选择较多的四个 DevOps 领域开源软件（Ansible、Jenkins、Go CD、Chef）进行扫描，结果显示：Jenkins 和 Go CD 中暂未发现使用传染性许可证的开源组件，Ansible 发现 1 个使用 GLP 的开源组件，Go CD 发现 3 个使用 GLP 的开源组件和 1 个使用 LGPL 的开源组件。

图 28 DevOps 领域热门开源软件许可证情况调查



软件名称	许可证类型	组件名称（带有传染性的许可证名称）
Ansible	GPL-3.0	ansible(GPL-3.0)
Jenkins	MIT	/
Go CD	Apache-2.0	codexmapping(GPL-2.0) tesnuke(GPL-2.0) git(GPL-2.0+) kafs(LGPL-3.0)
Chef	Apache-2.0	/

数据来源:中国信息通信研究院

总体来看，开源软件许可证问题较为复杂，企业在引入包含带有传染性许可证的开源组件时，应特别注意相关传染性组件的源代码后续是否可能在二次开发中被修改，如可能涉及修改，应注意修改后的软件是否可能涉及对外分发（如：对外公开销售软件等）。以 GPL 许可证为例，使用依 GPL 开源的软件并涉及到修改和分发时，用户需要将后续修改代码开源，如未遵循开源许可证的要求，可能会构成违约给企业带来风险。

（二）安全风险

1、风险分析

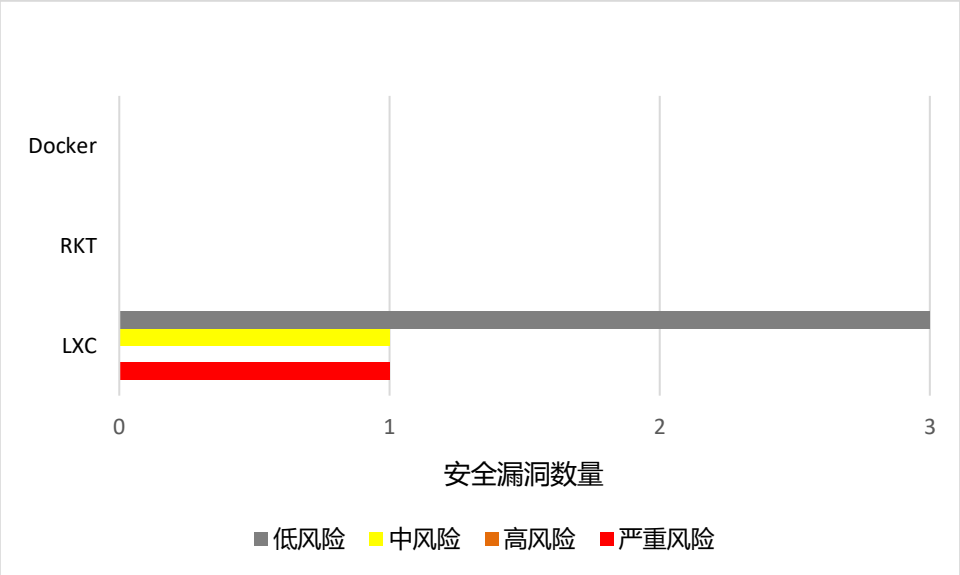
由于开源软件具有多人协作完成、开源许可证存在免责条款等特性，企业在使用开源软件时必须注意数据安全及隐私风险，若开源软件存有恶意代码、病毒或造成隐私泄露，将给使用者带来较为严重的危害。

总体来看，开源软件存在的安全问题较为严重，安全漏洞是主要的问题，后门等问题同样存在。开源软件的安全缺陷密度较高，据 SNYK 发布的《2019 年开源安全现状调查报告》显示，过去两年内应用程序的漏洞数量增长了 88%，仅 2018 年 NPM 的漏洞数量增长了 47%。系统信息泄露、密码管理、资源注入、跨站请求伪造、跨站脚本、HTTP 消息头注入、SQL 注入、越界访问、命令注入、内存泄漏是开源软件主要的安全风险。本次调查对部分热门开源软件进行了代码安全扫描，所用漏洞库与美国国家漏洞库（NVD）保持同步。

2、调查结果

热门开源容器运行技术中，LXC 存在漏洞问题，Docker 和 RKT 暂未发现漏洞。本白皮书对企业选择最多的三个开源容器运行技术（Docker、RKT 和 LXC）进行安全漏洞扫描，结果显示： LXC 中包含 1 个严重风险漏洞，1 个中风险漏洞以及 3 个低风险漏洞。

图 29 热门开源容器技术安全漏洞情况调查



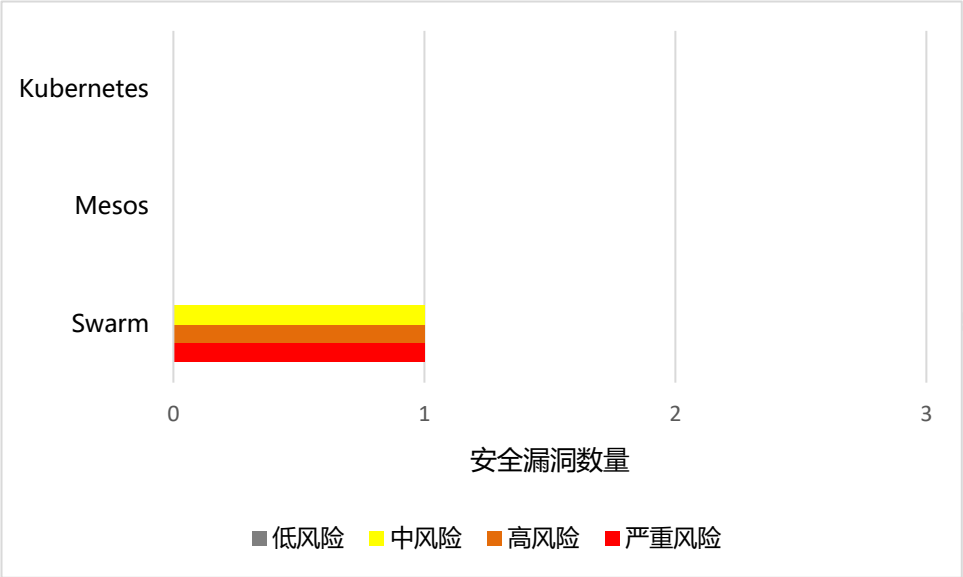
软件名称	严重风险	高风险	中风险	低风险
LXC	CVE-2016-8649	/	CVE-2015-1331	CVE-2017-5985 CVE-2015-1335 CVE-2015-1334

数据来源:中国信息通信研究院

热门开源容器编排技术中，Swarm 漏洞问题突出，Kubernetes 和 Mesos 暂未发现漏洞。本白皮书对企业选择最多的三个开源容器编排技术（Kubernetes、Mesos 和 Swarm）进行安全漏洞扫描，结果显示：Swarm 中包含 1 个严重风险漏洞，1 个高风险漏洞以及 1 个中风险漏

洞。

图 30 热门开源容器编排技术安全漏洞情况调查

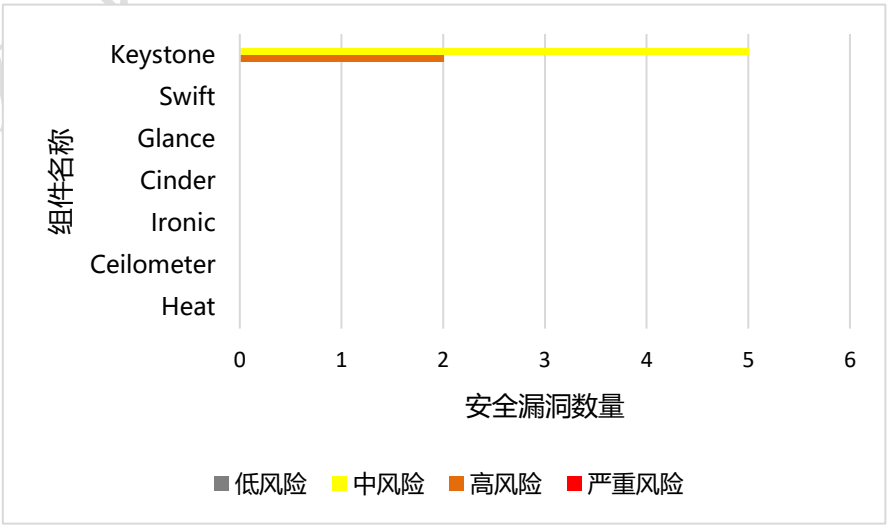


软件名称	严重风险	高风险	中风险	低风险
Swarm	CVE-2018-1002105	CVE-2019-9946	CVE-2019-1002100	/

数据来源:中国信息通信研究院

OpenStack 的 7 大常用组件中只有 Keystone 发现漏洞问题。本白皮书对 7 个 OpenStack 常用组件进行扫描，结果显示：Keystone 包含 2 个高风险漏洞，5 个中风险漏洞。其他几个常用组件暂未发现漏洞。

图 31 OpenStack 常用组件安全漏洞情况调查

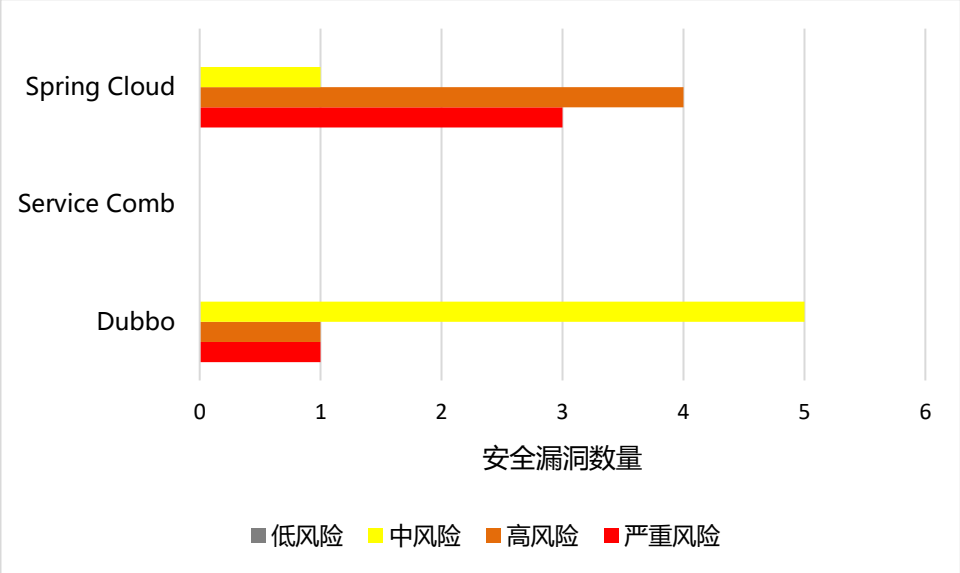


软件名称	严重风险	高风险	中风险	低风险
Keystone	/	CVE-2015-5162 CVE-2011-3147	CVE-2016-0757 CVE-2014-7230 CVE-2014-7231 CVE-2016-2140 CVE-2017-16239	/

数据来源:中国信息通信研究院

热门开源微服务框架隐含安全风险，其中 Dubbo 和 Spring Cloud 存在漏洞问题，Service Comb 暂未发现漏洞。本白皮书对企业选择最多的三个开源微服务框架技术（Dubbo、Service Comb 和 Spring Cloud）进行安全漏洞扫描，结果显示：Dubbo 包含 1 个严重风险漏洞，1 个高风险漏洞和 5 个中风险漏洞；Spring Cloud 包含 3 个严重风险漏洞，4 个高风险漏洞和 1 个中风险漏洞。

图 32 热门开源微服务框架安全漏洞情况调查



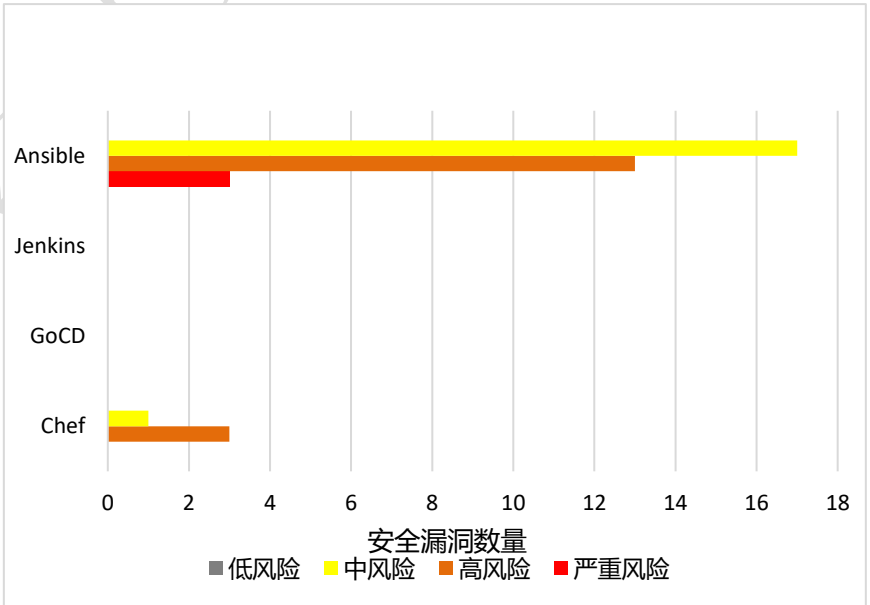
软件名称	严重风险	高风险	中风险	低风险
Dubbo	CVE-2018-17190	CVE-2018-11804	CVE-2018-11770	/

			CVE-2018-1334 CVE-2018-8024 CVE-2018-11760 CVE-2017-7678	
Spring Cloud	CVE-2018-19486 CVE-2016-2324 CVE-2016-2315	CVE-2018-11233 CVE-2018-11235 CVE-2017-1000117 CVE-2018-1000021	CVE-2017-15298	/

数据来源:中国信息通信研究院

DevOps 领域热门开源软件中，Ansible 和 Chef 存在较为严重的漏洞问题，Jenkins 和 Go CD 暂未发现漏洞。本白皮书对企业选择较多的四个 DevOps 领域开源软件（Ansible、Jenkins、Go CD、Chef）进行安全漏洞扫描，结果显示：Ansible 包含 3 个严重风险漏洞，13 个高风险漏洞，17 个中风险漏洞；Chef 包含 3 个高风险漏洞和 1 个中风险漏洞。

图 33 DevOps 领域热门开源软件安全漏洞情况调查



软件名称	严重风险	高风险	中风险	低风险
Ansible	CVE-2016-5008 CVE-2017-1000153 CVE-2017-1000154	CVE-2012-4541 CVE-2013-0269 CVE-2013-2633 CVE-2013-1844 CVE-2015-7815 CVE-2015-7816 CVE-2017-1000133 CVE-2017-1000151 CVE-2018-1064 CVE-2013-4969 CVE-2017-2295 CVE-2017-1000148 CVE-2017-14163 CVE-2019-10132	CVE-2017-1000155 CVE-2017-1000157 CVE-2016-10376 CVE-2017-14752 CVE-2017-15273 CVE-2017-10689 CVE-2017-5602 CVE-2017-9551 CVE-2016-8889 CVE-2019-3840 CVE-2014-3248 CVE-2014-3672 CVE-2015-5247 CVE-2017-1000131 CVE-2017-1000141 CVE-2017-1000156 CVE-2017-10690	/
Chef	/	CVE-2009-4014 CVE-2009-4015 CVE-2009-4013	CVE-2014-4616	/

数据来源:中国信息通信研究院

三、我国开源产业发展特点及趋势

科技类企业率先布局开源生态。开源逐渐成为科技公司抢占市场的有力机制，借助开源推广用户侧的事实标准，通过开源机制实现科技类公司的市场布局，建立上下游合作机制，扩大产业生态。我国科技类公司在跟随国际顶级开源项目的同时，积极推广自发开源项目，阿里、腾讯、华为、滴滴等科技公司纷纷成立开源管理办公室，负责公司对外开源的统筹规划，进行开源之前的合规检查及后续运营推广。截至 2019 年，阿里对外开源 150 个项目，腾讯对外开源 69 个项目。

开源的行业属性逐渐显现，开源用户尝试影响开源生态。国际顶级开源基金会多由软件厂商、硬件厂商等科技类公司重点参与，开源项目不一定完全解决用户实际生产需求，开源用户迫切需要加入开源生态并影响开源项目的发展走势，以满足用户实际生产需求。国际上已经成立 FINOS，开展金融领域的开源推进，拥有 30 余家会员单位、70 余个项目正在孵化；国内方面，中国信通院已经联合浦发银行等 10 余家金融机构及华为、腾讯等多家科技公司，共同成立了金融行业开源技术应用社区，孵化特定行业开源项目。

产业界逐渐关注开源风险问题，积极探索治理模式。近两年，开源许可证变更事件频繁发生，我国企业对开源的风险问题逐渐关注，认识到开源存在知识产权，需要关注合规问题，同时有一定的使用规则和允许的商业模式，企业需要事前摸清在哪些场景能够使用开源，会产生哪些额外的费用和投入，我国对开源的认识由盲目的引入转变为理性的引入，积极探索治理模式，应对开源风险。

四、我国开源产业发展建议

企业应树立开源风险意识，通过开源治理提升合规水平。1）通过开源知识培训等形式向企业相关人员灌输正确的开源理念，针对开源的概念、开源许可证的要求进行解读，明确开源可能涉及的风险，树立企业的开源风险意识。2）从管理角度搭建企业开源治理组织架构，设置明确的开源治理分工，将开源软件审核和风险控制的工作和责任具体落实到个人，并配备开源知识产权、法务、安全等人员协助推进开源软件合规使用。3）通过制定开源管理制度，建设企业内部开源软件管理平台，从公司层面对开源软件的引入和输出进行管理，构建全流程的企业级开源治理体系。

第三方机构宜组织推广国内开源项目，搭建开源配套基础设施，进一步推进标准制定。1）通过搭建国内开源共享和交流平台，营造更为开放的技术文化，帮助国内企业推广原创开源项目，扩大项目的行业影响力，链接科技企业与国内用户，推动国内开源生态健康、持续发展。2）针对当前国内尚未形成完整开源生态的现状，宜通过建设国内公开的代码托管平台、开源合规扫描工具、开源项目评价平台等开源配套基础设施，助力我国开源生态健康发展。3）针对国内开源产业相对缺少监管和规范的现状，中国信通院已经联合 30 余家金融机构和科技公司共同制定了开源软件治理的行业标准，进一步规范开源软件“申请-审批-使用”全流程管理，帮助企业建立自上而下的开源治理体系。

附录：开源软件风险调查扫描软件清单

许可证名称	许可证版本	下载地址
Ansible	2.7.10	https://github.com/ansible/ansible
Go CD	19.4.0	https://github.com/gocd/gocd
Jenkins	2.176.1	https://github.com/jenkinsci/jenkins
Chef	15.1.7	https://github.com/chef/chef
Docker	4.9.0	https://github.com/docker/docker-ce
LXC	2.0.11	https://github.com/lxc/lxc
RKT	1.30.0	https://github.com/rkt/rkt
Dubbo	2.7.1	https://github.com/apache/dubbo
Service Comb	0.3.0	https://github.com/apache/servicecomb-pack
Swarm	1.2.9	https://github.com/docker/swarm
Mesos	1.7.2	https://github.com/apache/mesos
Kubernetes	1.15.0	https://github.com/kubernetes/kubernetes